UDC 340
DOI 10.31733/2078-3566-2022-5-121-126

Liudmyla RYBALCHENKO©
Ph.D. (Economics),
Associate Professor
(Dnipropetrovsk State University of Internal Affairs, Dnipro, Ukraine)

Oleksandr KOSYCHENKO©
Ph.D. (Technics),
Associate Professor
(Dnipropetrovsk State University of Internal Affairs, Dnipro, Ukraine)

Illia KLINYTSKYI©
Graduate student
(University of Silesia, Katowice, Poland)

LEGAL REGULATION OF PERSONAL DATA PROTECTION IN THE COUNTRIES OF THE WORLD

Людмила Рибальченко, Олександр Косиченко, Ілля Кліницький. ПРАВОВЕ РЕГУЛЮВАННЯ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ В КРАЇНАХ СВІТУ. Відповідно до законодавства персональні дані – це відомості або сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована. Технологічний прогрес створює для суспільства дедалі ширший спектр потреб і можливостей, від бізнесу до політики. В останні роки збір і обробка персональних даних все частіше використовується в усіх сферах життя людини. Стрімкий розвиток інформаційних технологій вимагає використання персональних даних не лише для роботи, а й для повсякденного життя, приватного життя, медицини тощо. Є питання щодо порушення прав людини. Тому створення надійного захисту персональних даних від незаконного використання є актуальним для суспільства.

Створення належного рівня системи захисту персональних даних є одним із важливих завдань України на міжнародному просторі. Пріоритетним напрямком побудови державно-правового регулювання захисту прав і свобод суспільства, а також інтеграції до міжнародних та європейських стандартів є вдосконалення існуючої системи захисту персональних даних. Конфіденційність персональних даних захищена Конституцією України. Відповідно до законодавства України підприємства, установи, приватні компанії, банки та інші мають право обробляти персональні дані споживачів, при цьому вони зобов'язані захищати ці дані та несуть відповідальність за порушення їх конфіденційності.

Одним із шляхів запобігання порушенням прав людини на захист персональних даних є підвищення рівня обізнаності щодо правових засад обробки та захисту персональних даних. Запровадження у вітчизняне законодавство найкращих інструментів та європейських стандартів захисту персональних даних, посилення відповідальності за його порушення та моніторинг у сфері захисту персональних даних дасть можливість підвищити та посилити захист прав громадян на невтручання в особисте життя.

Ключові слова: *персональні дані, конфіденційність інформації, захист персональних даних, розвиток інформаційних технологій.*

© Rybalchenko L., 2022
ORCID iD: https://orcid.org/0000-0003-0413-8296
luda_r@ukr.net

© Kosychenko O., 2022
ORCID iD: https://orcid.org/0000-0002-6521-0119
kosichenko-inform@meta.ua

© Klinytskyi I., 2022
ORCID iD: https://orcid.org/0000-0002-7401-8233
illia.klinytskyi@us.edu.pl

Relevance of the study. The implementation of online services provides opportunities for convenient and quick collection and processing of information about a natural or legal entity. The use of personal data may be misused, illegally, which may lead to its leakage. The economic growth of the quality of life of Ukrainians, their well-being is an important component of the modern level of digitalization of society, implemented through electronic services, mobile applications, etc. Under such conditions, the vulnerability of privacy and confidentiality of personal data becomes a frequent phenomenon for violating the rights and freedom of a citizen. Illegal publication of personal data imposes responsibility on violators in accordance with the legislation of Ukraine.

The legislation of Ukraine defines the obligation of the owners to ensure the protection of personal data against accidental loss, destruction, illegal processing and illegal access to them. In Ukraine, the key document in the field of personal data protection is the Constitution of Ukraine [1], the Law of Ukraine "On the Protection of Personal Data" [2] and documents in the field of personal data protection, the Law of Ukraine "On Access to Public Information" [3], the Law of Ukraine "About information" [4]. Many other legal acts also contain provisions regulating the processing of personal data. The collection, storage, use and distribution of confidential information about a person who has not given consent to its processing is prohibited. Exceptions are cases that are defined by law and act in the interests of national security, economic well-being and human rights.

Article 32 of the Constitution of Ukraine [1] states that no one can interfere in personal and family life. Article 6 of the Law of Ukraine "On the Protection of Personal Data" [2] states that "personal data is processed for specific and lawful purposes, determined with the consent of the subject of personal data, or in cases provided for by the laws of Ukraine, in the manner established by legislation". According to Article 5 of the Law of Ukraine "On Protection of Personal Data", personal data can be classified as confidential information about a person by law or by the relevant person [2]. The issue of information security is related to information technologies that are used to ensure information security. Protection of information security consists not only in the application of unauthorized access to information, but also in the use of appropriate methods for its security and protection [14].

Recent publications review. The study of theoretical and practical aspects of personal data protection and information security dedicated to the works of Ukrainian scientists: O. Bodruk, V. Horbulin, V. Krysachenko, O. Manachinskyi, B. Parakhonskyi, T. Starodub, O. Shevchenko, O. Vlasyuk and others. Conceptual problems of information security were investigated by domestic and foreign scientists: R. Aron, K. Clausewitz, K. Hajieva, B. Liddell-Hart, N. Machiavelli, H. Moltke, K. Popper, P. Proudhon, E. Rybkin, S. Tyushkevich, M. Tsyurupa, A. Schweitzer, and others. No matter of wide number of reseaches, personal data protection and information security as scientific field is still in the conditions of the formation and requires more attention.

The article's objective is to systemize and analyze the legal regulation of personal data protection in the the foreign countries and Ukraine.

Discussion. January 28 is recognized as the International Day of Personal Data Protection. Data Protection Day is celebrated in all countries and in European countries. The establishment of such a day is related to the fact that network users do not forget to observe the rules of behavior on the Internet, which help to secure their virtual and real life and to improve the legal regulation of personal data protection at the international level.

For legal regulation in the field of personal data protection, the European Union has developed a regulation on the protection of personal data (General Data Protection Regulation, GDPR, hereinafter – the Regulation), which entered into force on May 25, 2018 [5]. According to the provisions of the Regulation, personal information is information that identifies, relates to, describes, can be linked directly or indirectly to a specific data subject or household.

The deepening of cooperation between Ukraine and the EU in the field of personal data protection is stipulated precisely in our national legislation. If it is necessary to transfer data from the EU to Ukraine, companies sign a document called Standard Contractual Clauses (SCC), which is the proper basis for data transfer in this case. In June 2021, a new version of the SCC was adopted. In June 2018, the law on the protection of personal data was signed in the USA. California Governor Jerry Brown signed the California Consumer Privacy Act 2018 (the "Act") [6]. This Privacy Act includes data security that is important to the safety and well-being of the people of California and the entire nation's economy. It should be noted that the California Consumer Privacy Act is a "victory" and a big step forward in the protection of personal data in

the United States. The Act provides new privacy rights for California consumers, including:

– the right to know about the personal information the company collects about them and how it is used and shared;

– the right to delete personal information collected from them;

– the right to refuse the sale of your personal information;

– the right to non-discrimination to exercise their rights under the CCPA [6].

Many well-known companies pay special attention to the protection of personal data. Thus, the Cisco company, with its obligations, respects the protection of the confidentiality of personal data of its employees, clients, business partners and other interests [9]. For whom, Cisco has run a global privacy program so that I can enforce and uphold high standards of privacy, selection, disclaimer, voice, privacy, privacy, transmission of personal data, and access to them of those other forms. Under the hour of collecting personal data from the entire world, Cisco is subject to ambush, which is designated by the global privacy policy. It expands on personal data, as it is processed by Cisco in the world, like electronic means, so in a familiar look, on paper wear.

The Global Privacy Policy, together with the Global Privacy Policy, the European Privacy Policy and the Business Personal Data Privacy Policy, are also intended to implement appropriate safeguards for the processing of personal data entrusted to Cisco and transferred from countries whose laws require adequate protection. This enables Cisco to share personal data globally. The general principles that establish Cisco's practices regarding the collection, use, disclosure, storage, protection, transfer, access, and other processing of personal data are as follows: authenticity, purpose limitation, proportionality, data integrity, data storage and deletion, data protection, rights of data subjects and reporting [9].

From July to September 2021, European data protection regulators (DPAs) imposed the 2 largest fines for GDPR violations:

– the Luxembourg DPA imposed a €746 million fine on Amazon (it is believed that the reason for the fine is Amazon's use of targeted advertising without proper user consent);

– the Irish DPA imposed a €225 million fine on WhatsApp due to data transparency issues.

These cases confirm a general trend – the efforts of regulators to force large companies to follow uniform rules and prevent another mass abuse during data processing.

The rapid development of information technologies takes place with large volumes of data processing, which is related to personal data, state institutions, banks, supermarkets, mobile communication devices, etc.

The functions of monitoring compliance with the legislation on the protection of personal data have been transferred to the Commissioner for Human Rights of the Verkhovna Rada of Ukraine. The processing of personal data on racial or ethnic origin, political, religious or ideological beliefs, membership in political parties and trade unions, criminal convictions, as well as data related to health, sexual life, biometric or genetic data is prohibited. The processing of these categories of personal data should take place only in exceptional cases with the provision of higher standards of both protection and compliance with the rights of the subjects of personal data. Previously, all personal data, with the exception of depersonalized data, was considered information with limited access. According to the new version of the law, information about receipt of budget funds, state or communal property by an individual in any form does not belong to information with limited access.

Indicative is the attitude towards the protection of personal data in Estonia [7], where each of its citizens has their own online account, in which they can track all requests for their personal data and know who, when and for what purpose applied to them. If a person believes that the request was unreasonable, he can file a complaint with the Personal Data Protection Inspectorate. Employees of the inspection have the right to check all state authorities for compliance with the rules of personal data protection. Since the adoption of the GDPR (General Data Protection Regulation) in Estonia, no violations and fines have been recorded. Estonia's cyber security strategy is based on 4 principles:

1) The protection and promotion of fundamental rights and freedoms in cyberspace and in the physical environment are equally important;

2) Measures to support cyber security in Estonia are considered as a stimulator of the speed of digital development, which is the basis of the socio-economic growth of the country. Security must support innovation, and innovation must support security;

3) Ensuring the security of cryptographic solutions is of unique importance to Estonia, as

it is the foundation of the digital ecosystem;

4) Transparency and public trust in the state are important for a digital society. Therefore, Estonia undertakes to adhere to the principle of open public communication.

In addition to the Ministry of Defense of Estonia, national cyber defense is supported by the Cyber Defense Division of the Estonian Defense League, a unit that includes cyber security experts from both public and private institutions [7].

According to the NCSI (National Cyber Security Index) in 2021, the leaders of the level of the national cyber security index in the world were: Greece (96.1), Lithuania (93.51), Belgium (93.51), the Czech Republic (92.21) and Estonia (90,91). Regarding the level of cyber security, Estonia (99.48) ranks 2nd after the United Kingdom (99.54) in the global cyber security index among European countries in 2021 [10, 11].

In Estonia, the legal regulation of information security is provided by the Constitution of Estonia, the Law "On Public Information", the Law "On Protection of Private Data", the Law "On Cyber Security", Cyber Security Strategy for 2019-2022. Estonia's level of information security has been tested by critical situations and has shown its efficiency and effectiveness. All state bodies and private structures of the country systematically interact with each other to prevent and overcome negative consequences. The Estonian experience shows that the issue of regulating information security requires balanced multifaceted solutions.

In France, the control of compliance with the legislation in the field of personal data protection is entrusted to the National Commission for Informatization and Freedoms (Commission Nationale de l'informatique et des Libertés, CNIL) [8]. CNIL is an independent administrative body with state funding, the main task of which is to ensure compliance with human rights, inviolability of private life, and protection of personal or public freedoms in the process of implementation and use of information technologies [8]. The decision of the CNIL can be appealed in the administrative court.

The activity of the French special-purpose state bodies in the field of information security is a component of measures aimed at the implementation of three main tasks inherent in special services: diplomatic intelligence, military defense and protection of economic interests. Individual issues of information security of the state are entrusted to one of the main intelligence agencies – the General Directorate of External Security (La Direction generale de Ia securite exterieure, DGSE), which is subordinate to the Ministry of Defense [8].

Looking at the statistics in the field of personal data protection, one can see that in recent years there has been an increase in the number of appeals received to the Authorized Body regarding violations in the field of personal data protection [13].

Table 1

Violations of personal data protection

Years	Appeals received	Inspections have been carried out	Prepared protocols
2014	928	53	8
2015	638	62	3
2016	1306	76	5
2017	1211	45	34
2018	806	41	14
2019	1061	36	10
2020	2031	67	9

The value of appeals is growing at the same time as the pace of digitization is growing and in the context of a pandemic, when the volumes and risks of personal data processing are growing. Therefore, in the near future, we can reasonably expect an increase in the number of appeals to these mechanisms and their activation.

The transfer of personal data between subjects, owners and managers located in different states is becoming increasingly relevant in the digital economy. Art. 28 of the Law of Ukraine "On the Protection of Personal Data" provide that "violation of the legislation on the protection of personal data entails responsibility established by law". In addition, administrative responsibility for violations in the field of processing and protection of personal data is established by Art. 188-39 of the "Code of Ukraine on Administrative Offenses" [13, 14]. Regarding the EU, according to Article 45 of the Regulation, the transfer of personal data is possible without restrictions: "if the European Commission has decided that a third country, a

territory or one or more defined sectors within such a third country, or a relevant international organization provides an adequate level of protection". As of today, the European Commission has recognized Andorra, Argentina, Canada (certain types of organizations), Faroe Islands, Guernsey, Isle of Man, Israel, Jersey, New Zealand, Switzerland and Uruguay as such states. The transfer of personal data of EU citizens and residents to the USA is possible under a special regime [13-14].

Conclusions. Thus, in each country, appropriate legislative, regulatory documents and standards have been introduced, which are intended to regulate the protection of personal data, processing, liability for violations of protection and privacy rights.

The main risks associated with the use of modern information technologies are the irresponsibility of persons who, during processing, disclose personal data, do not ensure the integrity and confidentiality of information, lack of reliable protection of personal data against leakage and distribution.

The development of Ukrainian legislation on the protection of personal data was oriented towards European standards, which are presented in documents and international treaties of the Council of Europe and the EU. The analysis of the national legal framework on the protection of personal data shows that the legal protection of personal data in Ukraine is insufficient and needs to be updated and improved.

In the current legislation of Ukraine, the regulation of issues of responsibility for violations of personal data protection standards still needs to be refined and adapted to international standards.

Conflict of Interest and other Ethics Statements

The authors declare no conflict of interest.

References

1. Конституція України [Конституція України] № 254к/96-ВР від 28.06.1996. URL : https://zakon.rada.gov.ua/laws/main/254%D0%BA/96-%D0%B2%D1%80#Text. [укр.].

2. Закон України «Про захист персональних даних» № 2297-VI від 01.06.2010. URL : https://zakon.rada.gov.ua/laws/show/2297-17#Текст.

3. Закон України «Про доступ до публічної інформації» № 2939-VI від 13.01.2011. URL : https://zakon.rada.gov.ua/laws/main/2939-17#Текст.

4. Закон України «Про інформацію» № 2657-XII від 02.10.1992. URL : https://zakon.rada.gov.ua/laws/main/2657-12#Текст.

5. General Data Protection Regulation (GDPR). Official Legal Text. URL : https://gdpr-info.eu.

6. California Consumer Privacy Act 2018. URL : https://oag.ca.gov/privacy/ccpa.

7. Estonian Defense League Cyber Unit. URL : https://www.kaitseliit.ee/en/cyber-unit.

8. Національна комісія з питань інформатизації та свобод (Commission Nationale de l'informatique et des Libertés, CNIL). URL : https://pidru4niki.com/82905/politologiya/diyalnist_spetsialnih_sluzhb_pravoohoronnih_organiv_frantsiyi_sferi_zabezpechennya_informatsiynoyi_bezpeki.

9. Глобальна політика забезпечення конфіденційності компанії Cisco [Cisco Global Privacy Policy]. URL: https://www.cisco.com/c/uk_ua/about/trust-center/global-privacy-policy.html. . [укр.].

10. Global Cybersecurity Index 2020. International Telecommunication Union. Development Sector. 2020. P. 172.

11. Гребенюк А. М., Рибальченко Л. В., Прокопов С. О. Моніторинг кіберінцидентів хмарних сервісів та захист цифрових каналів зв'язку. *Європейський науковий електронний журнал.* 2022. 3(18). С. 40-53.

12. Rybalchenko L., Kosychenko O. Economic security of Ukraine and ways of its increase. Innovative Wirtschaft und Management in der modernen Welt. Monografische Reihe "Europäische Wissenschaft". Germany. Buch 4. Teil 11. 2021. P. 109-123.

13. Бем М., Городиський І. Захист персональних даних: правове регулювання та практичні аспекти. Захист персональних даних: правове регулювання та практичні аспекти. Науково-практичний підручник]. 2021. 160 с.

14. Rybalchenko L., Kosychenko O., Klinytskyi I. Ensuring economic security of enterprises taking into account the peculiarities of information security. *Philosophy, Economics and Law Review.* 2022. 2(1). P. 71-81.

Submitted: 29.11.2022

1. Konstytutsiya Ukrayiny [Constitution of Ukraine] № 254k/96-VR from 28.06.1996. URL : https://zakon.rada.gov.ua/laws/main/254%D0%BA/96-%D0%B2%D1%80#Text. [in Ukr.].

2. Zakon Ukrayiny "Pro zakhyst personal'nykh danykh" [Law of Ukraine "On Personal Data Protection"] № 2297-VI from 01.06.2010. URL : https://zakon.rada.gov.ua/laws/show/2297-17#Text. [in

Ukr.].

3. Zakon Ukrayiny "Pro dostup do publichnoyi informatsiyi" [Law of Ukraine "On Access to Public Information"] № 2939-VI from 13.01.2011. URL : https://zakon.rada.gov.ua/laws/main/2939-17#Text. [in Ukr.].

4. Zakon Ukrayiny "Pro informatsiyu" [Law of Ukraine "On Information"] № 2657-XII from 02.10.1992. URL : https://zakon.rada.gov.ua/laws/main/2657-12#Text. [in Ukr.].

5. General Data Protection Regulation (GDPR). Official Legal Text. URL : https://gdpr-info.eu

6. California Consumer Privacy Act 2018. URL : https://oag.ca.gov/privacy/ccpa

7. Estonian Defense League Cyber Unit. URL : https://www.kaitseliit.ee/en/cyber-unit

8. National Commission on Informatization and Freedoms (Commission Nationale de l'informatique et des Libertés, CNIL). URL : https://pidru4niki.com/82905/politologiya/diyalnist_spetsialnih_sluzhb_pravoohoronnih_organiv_frantsiyi_sferi_zabezpechennya_informatsiynoyi_bezpeki. [in Ukr.].

9. Hlobal'na polityka zabezpechennya konfidentsiynosti kompaniyi Cisco [Cisco Global Privacy Policy]. URL : https://www.cisco.com/c/uk_ua/about/trust-center/global-privacy-policy.html. . [in Ukr.].

10. Global Cybersecurity Index 2020. International Telecommunication Union. Development Sector. 2020. P. 172.

11. Hrebenyuk, A. M., Rybal'chenko L. V. Prokopov S. O. Monitorynh kiberintsyndentiv khmarnykh servisiv ta zakhyst tsyfrovykh kanaliv zv″yazku [Monitoring of cyber incidents of cloud services and protection of digital communication channels] The First Special Humanitarian Issue of Ukrainian Scientists. *European Scientific e-Journal*. 2022. 3(18). P. 40-53. [in Ukr.].

12. Rybalchenko L., Kosychenko O. Economic security of Ukraine and ways of its increase. Innovative Wirtschaft und Management in der modernen Welt. Monografische Reihe "Europäische Wissenschaft". Germany. Buch 4. Teil 11. 2021. P. 109-123. [in Germ.].

13. Bem M., Horodys'kyy I. Zakhyst personal'nykh danykh: pravove rehulyuvannya ta praktychni aspekty. Naukovo-praktychnyy posibnyk [Protection of personal data: legal regulation and practical aspects. Scientific and practical textbook]. 2021. 160 p. [in Ukr.].

14. Rybalchenko L., Kosychenko O., Klinytskyi I. Ensuring economic security of enterprises taking into account the peculiarities of information security. *Philosophy, Economics and Law Review.* 2022. 2(1). P. 71-81.

ABSTRACT

According to the legislation, personal data is information or a set of information about a natural person who is identified or can be specifically identified. Technological progress creates an ever-widening range of needs and opportunities for society, from business to politics. In recent years, the collection and processing of personal data has been increasingly used in all spheres of human life. The rapid development of information technologies requires the use of personal data not only for work, but also for everyday life, private life, medicine, etc. There are questions about the violation of human rights. Therefore, the creation of reliable protection of personal data against illegal use is relevant for society.

Creating an appropriate level of personal data protection system is one of the important tasks of Ukraine in the international space. Improving the existing system of personal data protection is a priority direction for the construction of state and legal regulation of the protection of the rights and freedoms of society, as well as integration into international and European standards. Confidentiality of personal data is protected by the Constitution of Ukraine. According to the legislation of Ukraine, enterprises, institutions, private companies, banks and others have the right to process personal data of consumers, at the same time they are obliged to protect this data and are responsible for violations of their confidentiality.

One of the ways to prevent violations of human rights to the protection of personal data is to increase the level of awareness of the legal principles of processing and protection of personal data. The introduction of the best tools and European standards for the protection of personal data into domestic legislation, strengthening of responsibility for its violations and monitoring in the field of personal data protection will provide an opportunity to increase and strengthen the protection of citizens' rights to non-interference in their personal lives.

Keywords: *personal data, confidentiality of information, protection of personal data, development of information technologies.*